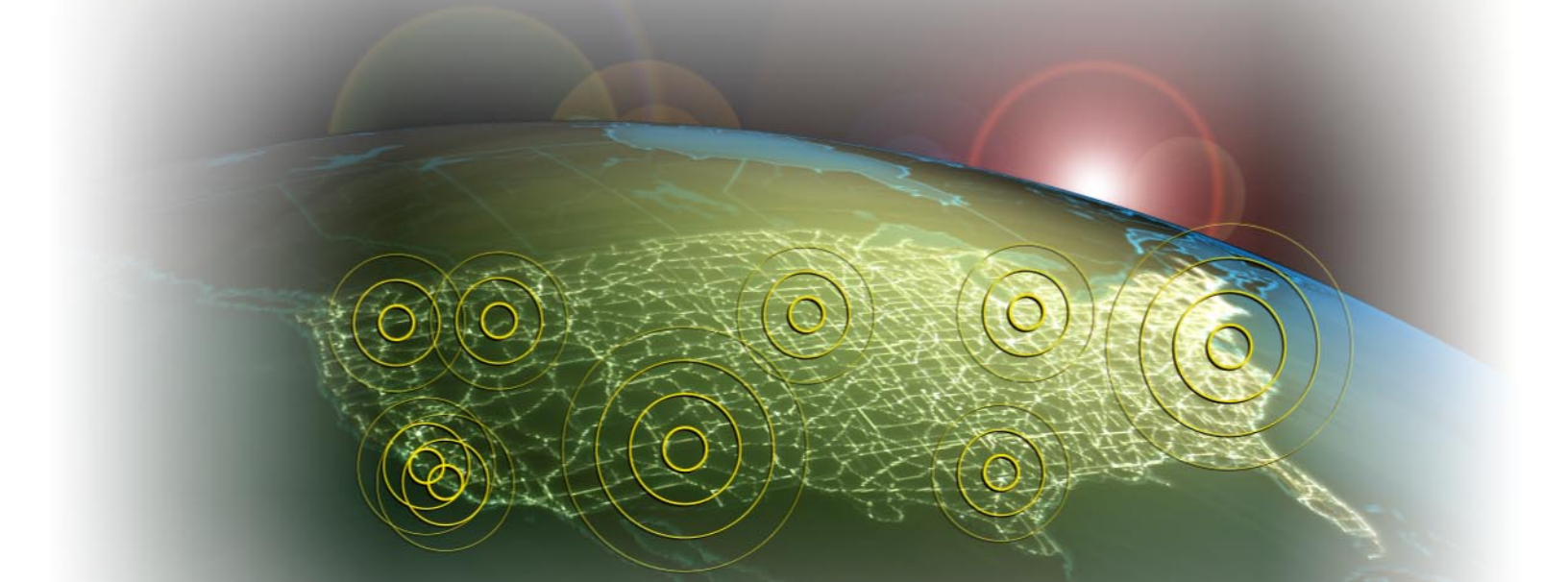
Securing the Power Flow



National Security

INL's SCADA Test Bed

Helping protect the nation's supervisory control and data aquisition systems.

The Invisible Threat

On August 14, 2003, many north-eastern metropolitan cities were in the midst of a historic blackout. According to the US-Canada Power Systems Outage Task Force, the event left millions of American and Canadian citizens without power for upwards of four days. It cost the U.S. economy between four and 10 billion dollars in lost wages, productivity and overtime. The event, though not terrorism related, brought infrastructure vulnerabilities to the forefront of homeland security. It proved that basic necessities needed for daily activity in our nation could be an easy target for cyber terrorists, hackers or disgruntled employees.

The security of control systems has been an issue of concern for the federal government since 9/11. In fact, the GAO report 04-354 states that an organization with sufficient resources, such as a foreign intelligence service or a well-supported terrorist group, could conduct a structured attack on the electric power grid electronically with a high degree of anonymity, and without having to set foot in the target nation. The blackout is only one example of the potential ramifications of a supervisory control and data acquisition, or SCADA attack. In fact, SCADA

Continued next page

INL Idaho National Laboratory

An INL electrician stands next to a set of modern gas circuit breakers. This set-up is part of the lab's comprehensive Critical Infrastructure Test Range.

Continued from front

systems and their components can be found in a number of national infrastructures including the water and oil and gas industry. SCADA systems are computer controlled devises that perform and relay physical changes in infrastructure systems to technical operators. They are capable of monitoring millions of data points simultaneously, and can therefore be manipulated by a cyber attack. The reality that an adversary could penetrate an electrical powergrid, or other control system, with little more than a laptop and an Internet connection, is a major threat to our way of life.

SCADA systems were originally designed for reliability and efficiency, not security. They were designed and put into place long before businesses relied on the Internet. Today, corporations use the Internet to monitor SCADA and other control system activity. Yet many prominent security flaws, including sub-par firewalls and non-unique passwords, continue to exist within these systems creating the potential for a devastating attack.

With prominent concerns such as these, the U.S. departments of Energy and Homeland Security selected Idaho National Laboratory to lead the nation in control system vulnerability reduction.

Full-Scale Testing

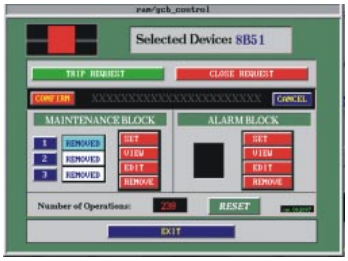
To help prevent an attack from occurring, INL established a SCADA Test Bed. A test bed is a functioning model of full or near full-scale proportions that allows individuals to visualize, analyze and test their control systems in a domain that is more realistic than computer simulation. Our SCADA Test Bed consists of several facilities that together create a centralized location for industry, equipment manufacturers and government agencies to work at finding tangible solutions to this growing threat. The Test Bed houses control systems from leading national and international manufacturers. Here, SCADA and cyber experts systematically examine the components of a functioning system and look for inherent vulnerabilities. Future testing and tool development will allow customers to bring their Remote Terminal Units (RTU), Intelligent Electronic Devices (IED), or Programmable Logic Controller (PLC) devices to the Test Bed and connect them to our full-scale electrical power grid. Our functioning power grid consists of 61 miles of 138 kV transmission loop distribution that feeds power to INL, and allows our technical staff to configure numerous network topologies to meet any customer's needs. Within the loop there

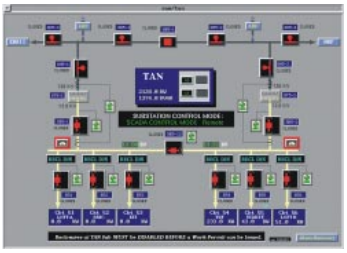
are multiple feeders, transformers and seven independent substations. These resources allow us to bring testing out of the theoretical, and into the real-world.

Customers have access to research and testing capabilities across a number of other INL Test Beds including our Wireless Test Bed which can simulate and test real TCP/IP, ATM, 802.11, GSM, and modem communication signals. The Wireless Test Bed, along with our other test beds, can be configured to communicate with a customer's SCADA systems via several means including ICCP, modbus, proprietary and public domain protocols, and DNP3. We also operate a specialized Cyber Test Bed where we can manipulate and test different firewall con-

Continued on back

A power management engineer stands next to oil circuit breakers located on INL's Critical Infrastructure Test Range.





INL acquired arc-resistant switchgear controlled by SCADA systems.

Continued from previous page

figurations and virtual private networks.

The resulting data provides individual answers and solutions tailored to each of our customer's needs. We work closely with other DOE national laboratories, allowing skilled specialists to work together to find solutions and improve security within their networks. This type of testing allows customers to visualize the impact of a real SCADA attack without the consequences to their operational systems. More importantly, it allows us to formulate practical, cost-effective solutions for the development of next generation systems.

INL Facilities

Situated on 890 square miles of isolated landscape, the INEEL has designed, built and relied on our own control systems for more than 50 years. The immense location requires the lab to operate and maintain a vast network of control systems for electrical, water and telecommunication distribution. Using this existing setup and system expertise, INL developed a Test Range to perform real world control system tests and attacks. Our Test Range includes the SCADA Test Bed, Wireless Test Bed, Cyber Test Bed and many others. Customers of the SCADA Test Bed have the ability to connect their systems to other components of our Test Range, allowing for a complete and thorough assessment.

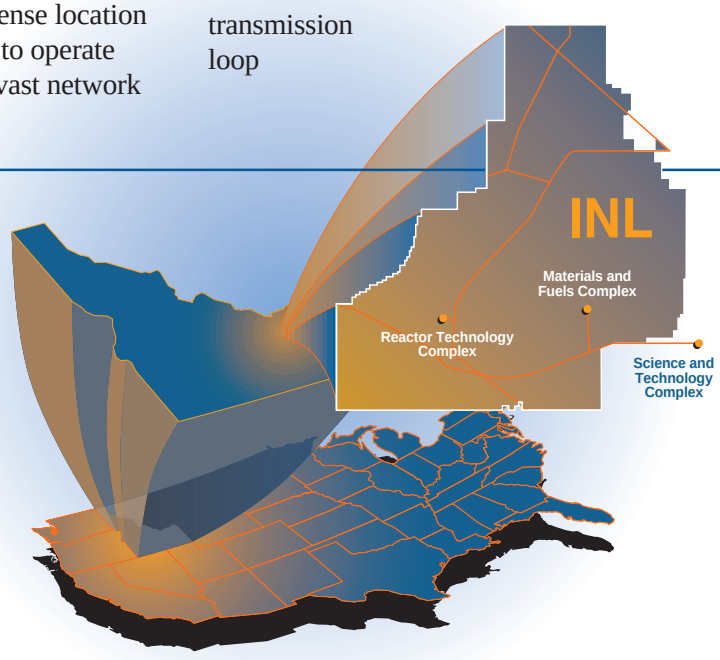
INL has established cooperative research agreements and non-disclosure agreements with dozens of companies, and is working with other companies that have expressed interest in the lab's capabilities.

INEEL Power Grid Quick Facts

- 61 miles of 138 kV transmission loop
- 13.8 kV distribution lines
- SCADA-controlled, dual-fed grid loop
- 7 substations, each can be isolated from the grid
- 3000 plus monitoring and control points in the system.
- Loop construction of the grid allows for other topologies configurations

INL SCADA Test Bed Capabilities

- Vulnerability assessments
- Comprehensive security training
- Tool development
- Virtual coordination with other DOE labs
- Access to multiple test beds



05-GA50139-02

For more information

Julio Rodriguez
208-526-2039 or
208-520-1645
Julio.Rodriguez@inl.gov

A U.S. Department of Energy National Laboratory